A NetDiscovery™ White Paper

First Steps for the *Homeland Security Information Sharing Act and the Mutual Assistance Convention*: global identifiers

Anthony M. Rutkowski[†]
VeriSign

Introduction

The terrorist attacks on 11 September 2001 revealed many critical inadequacies in the existing law enforcement and national security intelligence infrastructures. Over the decades, all kinds of information sharing impediments were both purposely and inadvertently introduced. The barriers rivaled the Berlin Wall among the diverse agencies – Federal, State, and Offshore. As incredible as it may seem, if two agencies had an electronic intercept on the same target party, they would likely not even know about each other.

On 19 November 2002 with a historic vote of the U.S. Congress, the intelligence cooperation walls were pulled down with the passage of the *Homeland Security Information Sharing Act*. This Act is actually Subtitle I of Title VIII of the better known *Homeland Security Act of 2002*. The HSIS Act also goes hand-in-hand not only with other provisions in the Homeland Security Act, but also with another key piece of new legislation passed on 15 November, the *E-Government Act of 2002*, The latter provides for "the management and promotion of electronic Government services and processes by...establishing a broad framework of measures..." for information sharing among law enforcement agencies. The E-Government Act includes the use of electronic signatures for secure transactions among agencies.

As industry and government work together to analyze and fix these inadequacies, those dealing with the effective gathering and exchange of intelligence information derived from electronic communication intercepts have come front-and-center. This is the primary focus of the *Homeland Security Information Sharing Act*.

In addition to these new U.S. domestic Federal Acts, the Council of Europe on 30 November 2000 updated the 40 year-old treaty on *Convention on Mutual Assistance in Criminal Matters*.[1] Clauses 12 and 13 of the Convention pertaining to the interception of telecommunications, allow for the first time the implementation of transnational interception orders. The provisions will likely come into force in early 2003 with the adoption by the eighth signatory country.

[†] Vice President for NetDiscovery Strategy tony@verisign.com. Chair, OASIS LI-XML Technical Committee. Acting President, Global LI Industry Forum www.gliif.org.

[1] Judicial cooperation in criminal matters: mutual Assistance in Criminal Matters between Member States, Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union [Official Journal C 197, 12.07.2000].

Such intelligence is known globally as Lawful Interception (LI). In the U.S. it is also referred to as Lawfully Authorized Electronic Surveillance (LAES). Diverse legal jurisdictions and agencies can institute such interception against criminal or terrorism suspects pursuant to different national and local law in the U.S. and worldwide. Increasingly - with international suspects being highly mobile and using advance network communication access and application technologies worldwide – these intercepts present complex legal and technical challenges.

One of the more significant impediments existing within the Lawful Interception industry is the complete lack of structured basic interception information identifiers on a global basis. These include the identity of the Law Enforcement Agency, the case identity, the communications services provider, and the network elements involved in an interception. The lack of such common basic identifiers effectively makes every action a "one-off" between the Law Enforcement Agency and the communications provider or agent supporting the interception. In many cases, the existing standards do not even allow global identifiers to be constructed. This significantly inhibits the thousands of different Law Enforcement Agencies in the U.S and worldwide from working together effectively at the most basic levels, including achieving the core objectives of the *Homeland Security Information Sharing Act* and the *Mutual Assistance Convention*.

This NetDiscovery™ White Paper discusses the situation today and points to a few simple steps designed to remove these impediments and bring about the compelling goal of the new U.S. and European Acts – sharing investigative information associated with lawful interception of communications by suspected terrorists or criminal suspects.

Basic Interception Identifiers – the challenge

fig. 1 Basic Interception Identifiers

All lawful interceptions anywhere in the world inherently involve four basic identifiers: 1) who is the law enforcement agency involved; 2) a reference designation for the investigative case interception; 3) the communications network provider who is effecting the interception; and 4) one or more "network elements" that have a binding to the case target, such as a telephone number, IP address, Email account, etc. All intercept related data and content information is tagged with these four identifiers plus a time stamp identifier – which in theory should enable interception information to be shared efficiently among law enforcement agencies and every level and worldwide.

Unfortunately, although most of these identifiers are called for in all telecommunication "handover" specifications for producing lawful interception information, any kind of effective sharing is effectively prevented because of several fundamental roadblocks:

a) no standards exist for structuring these identifiers for sharing,

b) no common mechanisms exist for creating and authenticating most of the identifiers involved - they are simply created ad hoc between each of the many thousands of Law Enforcement Agencies and each of the thousands of communication service providers, and

c) no requirements exist for law enforcement agencies, judicial authorities, and communication providers to use standard, globally-unique identifiers for their lawful interceptions.

As a result, even if agencies wanted to share information, there's no effective technical means of achieving it except though costly and burdensome individual processing on a large scale.

Interception Reference Identifiers: while we're at it

The four basic interception identifiers described above are always present as part of the instantiation of any lawful order or warrant and bound to the resulting information. Two other important identifiers are also often included as part of the interception information.

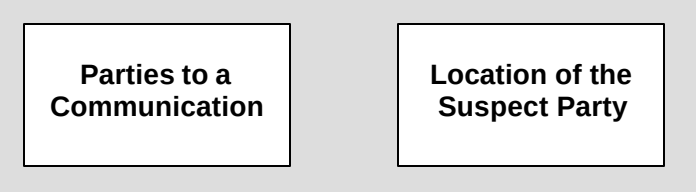

fig. 2 Reference Interception Identifiers

Parties to a communication and location information vary as to the kind of service involved and the ability to obtain the information – technically and legally. In general, the parties may include the communication originating party, the terminating party, forwarded-to party, call-waiting party, call-attempted party, and conferenced parties. For store-and-forward or PAM (presence and availability management) kinds of services, however, this may also involve the querying party.

Just like the basic interception identifiers, they are specified in all the "handover" specifications and face similar roadblocks – lack of common global structural standards for sharing the information. These will be treated in a subsequent NetDiscovery White Paper.

The Handover Specifications

Handover specifications are those which describe what intercepted communications information or content a communications provider is obliged to provide to a Law Enforcement Monitoring Facility, including the structure and process for conveying the information or content, i.e., interface and protocol. There are effectively two groups of standards in significant use today.

Only ETSI (European Telecommunication Standards Institute) standard ES 201 671 and its various derivatives[2] exist globally as Lawful Interception handover standards. This

[2] The phrase "ES 201 671 derivatives" here refers to the basic standard **Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications**

specification is used in almost every country worldwide outside North America. Within North America, TIA/EIA/IS-J-STD-025[3] and its various derivatives[4] - which were developed for CALEA[5] compliancy among telecommunication carriers in the U.S. – is significantly used in North America. Although CALEA applies only to a set of minimal capabilities telecommunication carriers are required to have in place, the size of this market makes J-STD-025 and its derivatives significant. Additionally, several proprietary specifications exist for vendor access, mediation, and collection equipment deployed by Law Enforcement Agencies.

The ETSI Standard

The ETSI ES 201 671 standard provides for a Handover Interface (HI) using three protocols designated ports HI1, HI1, and HI3 – respectively for administrative, signalling and content handovers from a communications provider to a Law Enforcement Monitoring Facility. The protocol specifies certain basic interception identifiers, as well as associated party identifiers.

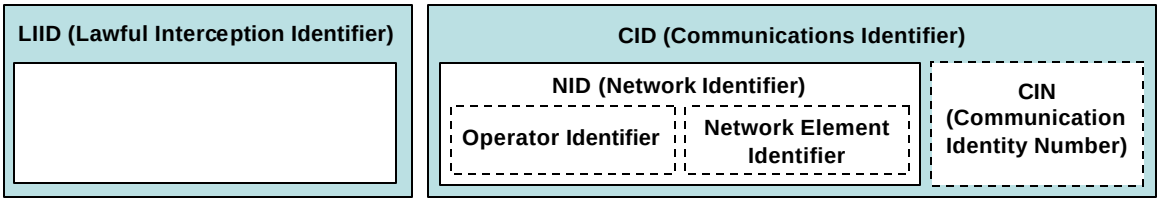

fig. 3 The ETSI ES 201 671 Specification for the Basic Identifiers

- **LIID (Lawful Interception IDentifier)**.[6] The LIID is in general a free-form identifier agreed between the LEA and the communications provider for each interception target. It is also occasionally referred to in the standard as the warrant reference number. The LIID format consists of alphanumeric characters (or digit string for sub-address option[7]). It might for example, among other information, contain a lawful authorization reference number, and the date, when the lawful authorization was issued. The LIID ASN.1 name is **LawfulInterceptionIdentifier**.
  - Notwithstanding all of the above, ES 201 671 specifies FTP as the means for transporting data across a HI2 or HI3 port, and then proceeds to specify a LIID format for naming files transported.
    - File naming method A (files that contain interception data only for one observed target) specifies that the LIID "has a character string (or digit string for sub-address option) value, e.g. 'ABCD123456'. This is a unique interception request identifier allocated by

---

traffic, version 2.1.1 (2001-09), current versions under development, and other ETSI Lawful Interception standards for wireless, cable and IP services, including similar national standards.

[3] TIA/EIA/IS = Telecommunications Industry Association, Electronic Industries Alliance, Alliance for Telecommunication Industry Solutions.

[4] The phrase "J-STD-025 derivatives" here refers to the basic standard **Lawfully Authorized Electronic Surveillance,** current versions under development, and other U.S. based standards bodies Lawful Interception standards for wireless, cable, and signalling services.

[5] Communications Assistance for Law Enforcement Act of 1994.

[6] Sec. 6.1 of ETSI ES 201 671 V2.1.1 specifies: "for each target identity related to an interception measure, the authorized NWO/AP/SvP operator shall assign a special Lawful Interception IDentifier (LIID), which has been agreed between the LEA and the NWO/AP/SvP. It is used within parameters of all HI interface ports." See fn. 8, below

[7] The option is applicable to certain kinds of ISDN interceptions.

the provider's Administrative Function (ADMF). It will be given by the ADMF to the LEA via the HI1 interface after the ADMF has been authorized to command the start of the interception of a specific target. The possible network operator identifier part[8] used should be agreed with (and allocated by) the regulatory organization administrating the local telecommunication practises."[9]

- File naming method B (when several targets' intercepted data is gathered to common delivery files) specifies use of "monolithic fixed format file names, e.g., ABXY00041014084400001, where ABXY = Source node identifier part, used for all files by the mobile network operator 'AB' from this MF node named 'XY,' 00 = year 2000, 04 = month April, 10 = day 10, 14 = hour, 08 = minutes, 44 = seconds, 0000 = extension, 1 = file type. The type '1' is reserved for IRI data files. (Codings '2' = CC(MO), '4' = CC(MT), '6' = CC(MO&MT) are reserved for HI3)."

- **CID (Communication Identifier)**.[10] A CID is used to designate specific communications of the target and used to correlation with any intercepted communications content. For the GPRS system, the CID is a combination of the GGSN (Gateway GPRS Support Node) and charging ID. The CID ASN.1 name is CommunicationIdentifier. The CID consists of two parts
  - **NID (Network Identifier)**. The Network IDentifier is a mandatory parameter; it should be internationally unique. Intercepting Node ID is used for the NID in the GSM system. The NID generally consists in one or both of the following two identifiers. It is mandatory that one of them is used. The NID ASN.1 name is **Network-Identifier**.
    - **Operator (NWO/AP/SvP[11]) identifier.** Unique identification of network operator, access provider or service provider. The ASN.1 name is **operator-Identifier** and its length is specified as a maximum of 5 octets.
    - **NEID (Network Element Identifier)** – usually an address of some sort, such as an E.164 international node number in the case of circuit switched networks, such as ISDN, PSTN, GSM; an X.25 address; an IP address. The ASN.1 name is **network-Element-Identifier** with a choice of four ASN.1 OID elements with a 25 octet maximum size.
      - **e164-Format**
      - **x25-Format**
      - **iP-Format**
      - **dNS-Format**
  - **CIN (Communication Identity Number)**. This is optional, except if for IRI in case of reporting events for connection-oriented types of communication (e.g. circuit switched calls), it is mandatory. It is a temporary identifier of an intercepted communication, relating to a specific target identity. The correlation number is used for the CIN for GSM interceptions. The CIN ASN.1 name is **communication-Identity-Number** and its length is specified as a maximum size of 8 octets.

In addition to the basic identifiers described above, the ETSI standard also specifies two important utility identifiers – one identifying the timing of the interception, and the second the delivery.

---

[8] In Europe, the two-character GSM Mobile Network Code is apparently the basis for the two digit specification.

[9] See ES 201 671 V2.1.1 at 60, 94-95.

[10] See Sec. 6.2 of ETSI ES 201 671 V2.1.1 "The CID distinguishes between the different activities of the target identity. It is also used for correlation between IRI records and CC connections. It is used at the interface ports HI2 and HI3."

[11] NWO/AP/SvP is a specialized term for communication provider within ETSI LI standards that stands for NetWork Operator/Access Provider/Service Provider.

TimeStamp. The ETSI LI time stamp is rigorously specified. The start and stop times of every intercepted communication are always required. These special time identifiers are critical to the discovery process. If two targets are communicating with each other, each target is dealt with separately. The parameter shall have the capability to indicate whether the time information is given as Local time without time zone, GMT with time zone, or UTC. Normally, the network provider defines these options.[12] UTC Time is an ASN.1 universal class and its format is the one defined in case b) of the ASN.1 recommendation [ITU-T, Rec. X.680] (year month day hour minutes seconds)[13] Local Time Stamp is specified in GeneralizedTime format - an ASN1 universal class and formatted in case a) of ASN.1 recommendation [ITU-T, Rec. X.680], and b) (year month day hour minutes seconds) with winterSummerIndication. Required precision is 1 second.[14] Additionally, ETSI has a Time Stamp Profile standard that provides the specifications for secure, authenticated time stamp clients and servers.[15]

Content Delivery Link Identifier. The delivery of the interception – if by a temporary (e.g., dialed) switched communication circuit – is specified by the CCLID (Communications Content link identifier). This identifier is only used at the interface ports HI2 and HI3 in case of the reuse of CC links. For each CC link, which is set up by the mediation function towards the LEMF, a CC link identifier (CCLID) is transmitted in the HI2 records and HI3 setup message in addition to CIN and NID. For the correct correlation of multiparty calls this identity number indicates in the IRI records of each multiparty call, which CC link is used for the transmission of the CC. The CCLID may use the same format as the CIN; in this case, it need not be transmitted explicitly during set up of the CC links, as part of HI3. The CIN may also implicitly represent the CCLID. The ASN.1 name is **CC-Link-Identifier**.

In addition to the above specifications, the ETSI ES establishes lengths for each identifier.[16]

Field	Minimum length (decimal digits)	Maximum length (decimal digits)	Maximum length (Half-Octets)
LIID	2	25	25 + 1
Operator ID	2	5	5 + 1
CIN	6	8	8 + 1
CCLID	1	8	8 + 1

The TIA J-STD

J-STD-025 provides for a handover "e-interface" and a single protocol designated LAESP for signalling handovers from a telecommunications carrier to a Law

[12] See D.5, Date & time, TimeStamp, ES201671 at 27.

[13] ES201671 at 71

[14] Id at Table F.3.5. p. 91.

[15] See Time stamping profile,ETSI TS 101 861 V1.2.1 (2002-03)

[16] See ES 201 671 V2.1.1 Table E.5.1 at 90.

Enforcement Monitoring Facility. The e-interface here is the equivalent of the ETSI HI2 port. The specified basic identifiers are similar, but given different data element names. They are depicted in their comparable relationships in Fig. 4, below.

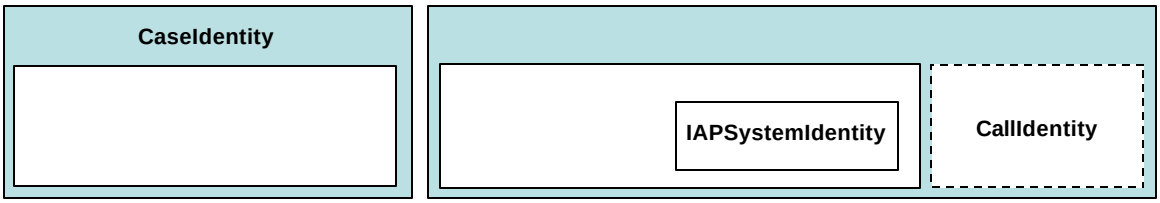

fig. 4 The J-STD-025 Specification for the Basic Identifiers

- **CaseIdentity**. The CaseIdentity parameter contains a case identity assigned by the LEA for a particular electronic surveillance. There is no further specification other than it may vary between 1 and 25 characters in length.[17] Otherwise it is a free-form format "designated by the LEA and provided to a TSP at the time of provisioning of an electronic surveillance."
- [Communication Identifier]
  - [Network Identifier]
    - **IAPSystemIdentity**. The IAPSystemIdentity identifies the system of the Intercept Access Point (IAP), e.g., CLLI code, "MSCID-12345-123" or "2025551234" (E.164 address of node). It should not imply the specific location of an intercept subject. Its size may vary between 1 and 15 octets in length.
- **CallIdentity.** The CallIdentity parameter is used to uniquely identify a particular call, call appearance, or call legs within the context of a single system. The CCOpen and Change messages can correlate the CallIdentity to one or more CCCs when content is delivered. It is include for circuit-mode calls to identify a particular circuit-mode call for the CCC. A unique call identity may be generated for the CCOpen Origination, TerminationAttempt, NetworkSignal or Change message which is used to correlate other messages with the delivered call content. CallIdentity is replaced with PDUType for packet-mode calls to identify the type of packet data units being intercepted (e.g., IP, PPP, X.25 LAPB, ISDN D-channel). A CallIdentity may be released for other uses with a Release or Change message. CallIdentity shall not be immediately re-used. HLRs and similar systems that do not correlate messages with CallIdentity(ies) do not need to release the CallIdentity. It is specified in ASN.1 as a sequence consisting of a sequenceNumber of 1 to 25 characters followed by an optional systemIdentity of 1 to 15 characters. This may occur when the system issuing the sequenceNumber is different than the accessing system, e.g., CLLI code, "MSCID-12345-123" or "2025551234" (E.164 address of node).[18]

Time Stamp. Like the ETSI standard, the J-STD also specifies a time stamp, albeit with minimal specificity. The "TimeStamp parameter identifies the date and time of access."[19] It is specified in GeneralizedTime – presumably referring to the ASN.1 parameter for local time. J-STD notes that this data element "permits an LEA to associate call-identifying information with the content of a call. A call-identifying message must be sent from the TSP's IAP to the LEA Collection Function…time-stamped to an accuracy of at least 200 milliseconds. This capability…requires time stamp accuracy for call events."[20]

---

[17] See Sec. 6.4.5. CaseIdentity, J-STD-025A at 74.

[18] See Sec. 6.4.4. CallIdentity, J-STD-025A at 74.

[19] See Sec. 6.4.13 TimeStamp, J-STD-025A at 78.

[20] See Sec.4.7 Timing Information, J-STD-025 at 31.

Content Delivery Link Identifier. The J-STD standard also specifies CCLID-equivalent specific specialized identifier for LI circuit switched networks, which is named a **CCCIdentity**. The CCCIdentity parameter identifies the Call Content Channel or pair of Call Content Channels used for conveying call content. Each channel is identified with a VisibleString which may contain a directory number (e.g., "202-555-1111"), a trunk identity (e.g., "FBITG-001" or "LAES-999"), an IP network address (e.g., "IP: 101.012.103.104:100") or an X.25 network address (e.g., "X121: 1234-5678901234"). The CCCIdentity can is between 1 and 80 octets in length.[21]

The TIIT Standard

The Netherlands Ministry of Justice standard for IP Intercepts designated TIIT provides the specification of the interface from an Interception Function within an IP network to a Law Enforcement Monitoring Facility (LEMF)[22] The interfaces cover HI1, HI2, and HI3 ports and the protocol is designated the "TIIT Protocol." The specified basic identifiers are similar, but given different data element names. They are depicted in their comparable relationships in Fig. 5, below.

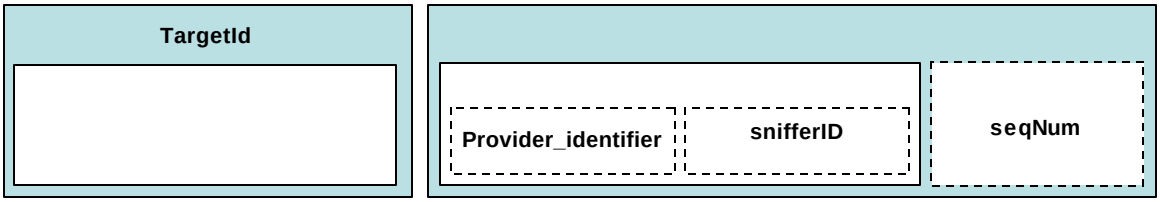

fig. 5 The TIIT Specification for the Basic Identifiers

- **TargetIdentifier**. The TargetID (ASN.1 name) is specified only as a MD5 hash generated by the LEMF. In this way a LEMF can generate its own identifiers, without compromising the interested LEA if the packet is intercepted en route.[23]
- [Communication Identifier]
  - [Network Identifier]
    - **provider_identifier**. The identifier provider identifier is a unique number that identifies a specific provider. It is defined as an unsigned 16 bit integer.
    - **snifferID**. A value determined by the Provider in order to distinguish between the different access devices.
- seqNum. The seqNum value will be incremented for every packet sent, whether the LEMF channel is available or not. The initial value of seqNum MUST be larger than 0x10. If wrap around of the value of seqNum should occur, the wrapped value MUST be smaller than 0x10.

Time Stamp. The TIIT standard has a simple schema based on unsigned integer seconds or microseconds since 1-Jan-1970 0:00 hours UTC.

---

[21] See Sec. 6.4.6 CCCIdentity, J-STD-025A at 75

[22] Directorate General for Telecommunication and Post of the Ministry of Economic Affairs (EZ), Transport of Intercepted IP Traffic , TIIT V1.0.0 (2002-09).

[23] 8.4 Target Identifier, id. at 14.

The Cable Labs PCESP Standard

The Cable Labs has developed a standard for Intercepts designated the PacketCable Electronic Surveillance Protocol (PCESP), which specifies the interface and an Interception Function within a DOCSIS 1.1 broadband access network to a Law Enforcement Monitoring Facility (LEMF) [24] The interfaces cover the equivalent of HI2 and HI3 ports. The specified basic identifiers are similar, but given different data element names. They are depicted in their comparable relationships in Fig. 6, below.

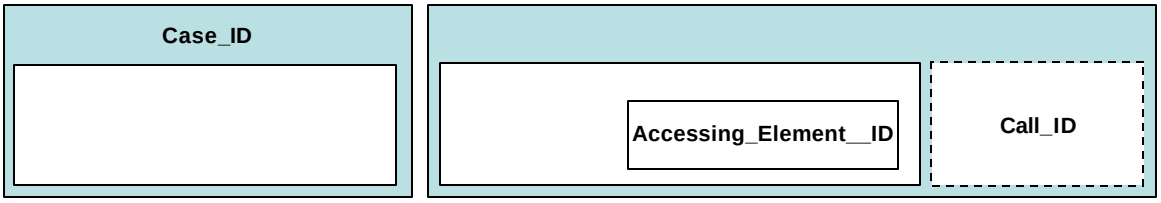

fig. 6 The PCESP Specification for the Basic Identifiers

- **Case_ID**. Identifies the Surveillance Subject.[25] It is specified between 1 and 25 characters in length.[26]
- [Communication Identifier]
  - [Network Identifier]
    - **Accessing_Element_ID**. Identifies the accessing element. It is specified between 1 and 15 characters in length.
- **Call_ID**. Uniquely identifies a call within a system. It consists of a sequencenumber VisibleString specified between 1 and 25 characters in length and a systemidentity between 1 and 15 characters in length. The Delivery Function generates this structure from the Billing-Correlation-ID (contained in the Event Messages) The sequencenumber is generated by converting the Timestamp (32 bits) and Event-Counter (32 bits) into ASCII strings, separating them with a comma. The systemidentity field is copied from the Element-ID field

Time Stamp. The PCESP standard specifies a time stamp named Event_Time. It identifies the date and time that the event was detected. Within a 200 millisecond accuracy, it identifies the time the event was detected by the Intercept Access Point.

---

[24] Cable Television Laboratories, Inc. (CableLabs ®)PacketCable™ Electronic Surveillance Specification, PKT-SP-ESP-I01-991229, December 29, 1999

[25] id. at 28.

[26] See Sec. 5.5.9 Message Parameters, id. at 37.

Toward a Global Interception Identifier Schema

For reasons that are largely historical, serendipity and the insularity of national bodies have conspired to erect barriers at the most basic level to the implementation lawful interceptions and sharing of information across national borders. The previous section of this White Paper makes it clear that comparable basic information identifiers for LI exist in every standard – with the ETSI ES201671 providing the most comprehensive core specifications, albeit still insufficient. However, from the table below, it can be seen how every standards body – even as to the ASN.1 names that should provide for interoperability – have constructed them differently.

Identifier	ES 201 671	J-STD-025	TIIT Standard	PCESP Standard
Law Enforcement Agency; Interception Reference	LawfulInterceptionIdentifier	CaseIdentity	TargetId	Case_ID
Communication Reference	CommunicationIdentifier Network-Identifier operator-Identifier network-Element-Identifier	IAPSystemIdentity	provider_identifier snifferID	Accessing_Element_ID
Content Link	communication-Identity-Number	CallIdentity	seqNum	sequencenumber systemidentity
Event Time	TimeStamp UTCTime GeneralizedTime	TimeStamp GeneralizedTime	[proprietary]	Event_Time
Content Delivery	CC-Link-Identifier	CCCIdentity		

The new U.S. and European Acts provide a compelling legal basis for developing a framework for harmonization and mutual use of a basic LI identifier schema. This includes making necessary adjustments to the existing specifications through liaison among the respective standards bodies. More importantly, what is urgently needed is the creation of a common global method for actually forming the identifiers together with a registry for the associated LEAs, judicial authorities, operators, and network elements who are part of the overall LI process. Fortuitously these are activities substantially within the scope of the newly created OASIS LI-XML Technical Committee.

Step 1 – Develop the global framework

The most important first step in this process involves the creation of a common framework among all the relevant LI parties on the next four steps. This doesn't imply that there is only a single worldwide body involved in this activity, nor a single way of creating identifiers. What is only necessary is that everyone will work together in a structured way to provide for global identifier uniqueness, to avoid incompatibilities, and to allow discovery, authentication, and consistent interpretation of everyone's identifiers as data elements.

There is considerable comparable work occurring in many other fields, there are excellent forums, precedents, and tools for bring this all about. The new legal mandates coming into force as well as funded programmes should provide additional incentives.

Step 2 – Agree on a specification for globally unique identifiers

In the previous section reviewing all the various existing standards, it was apparent that the actual process of creating identifiers has been largely a one-off phenomenon implemented between LEAs and operators or even individual employees around the world. Some structured way of creating these identifiers is needed. There can even be differing implementations in different venues – but they need exist and consistently followed and globally unique. They also must be useable across the two prevailing structured data syntax standards in the LI environment – ASN.1 and XML.

Some work along these lines has already occurred in the existing OASIS Court Filing Technical Committee, and its XML specification[27] has provides a structured base data element "fullCaseNumber" that "includes all qualifiers necessary to completely specify the case within its venue, to fix the court type, court location, category, year, number, etc."

This step must include a comprehensive effort to discover what practices exist on any kind of a widespread basis – internationally or nationally – for forming existing or similar LI basic identifiers.

Step 3 – Establish a global LI identifier registration and authentication mechanism

Once a schema for globally unique identifiers exists, a companion capability needs to be implemented. This includes both a validated identifier registry – a kind of master directory - for LEAs, courts, network service operators, and network elements - as well as a secure means of querying the registry for authentication purposes. In many ways, this capability resembles other Internet-based identifier systems, such as that used for domain names.

Like the Internet Domain Name System, registration and query mechanism can exist as a hierarchical, distributed schema. It can also provide a very important additional functionality – the public encryption keys by which all the parties and instruments associated with the Lawful Intercept process could be authenticated with a significant degree of trust.

Step 4 – Adjust the identifier specifications in existing standards

The several organizations involved in the LI standards development process should have a common interest in adjusting their basic identifiers to be globally unique and to facilitate exchange of information. The ETSI LI Technical Committee rapporteurs meeting 10-11 Dec at Mainz decided to adopt unique global identifiers to facilitate the implementation of the European Convention on Mutual Assistance. Other standards organizations should follow their lead.

It is also feasible for Lawful Intercept service bureaus to implement bridge mechanisms for the diverse specifications by effecting translations the different protocol specifications. This could expedite implementation among LEA end-user customers and

[27] See OASIS, Electronic Court Filing 1.1, Proposed Standard.

their collection system manufacturers until such time as the standards specifications are officially altered.

Step 5 – Get the parties in the LI process to begin using the tools

The last step may be the most difficult to completely implement. Changing practices completely at local levels could take many months or even years to implement. On the other hand, relatively few jurisdictions are responsible for most of the interceptions, and a mandate established at national levels could quickly make common LI identifiers a reality.